COUNTY OF LOS ANGELES
DEPARTMENT OF AUDITOR-CONTROLLER

KENNETH HAHN HALL OF ADMINISTRATION
500 WEST TEMPLE STREET, ROOM 525
LOS ANGELES, CALIFORNIA 90012-3873
PHONE: (213) 974-8301 FAX: (213) 626-5427

JOHN NAIMO
AUDITOR-CONTROLLER

October 28, 2016

TO: Supervisor Hilda L. Solis, Chair
Supervisor Mark Ridley-Thomas
Supervisor Sheila Kuehl
Supervisor Don Knabe
Supervisor Michael D. Antonovich

FROM: John Naimo
Auditor-Controller

SUBJECT: **DEPARTMENT OF MENTAL HEALTH – INFORMATION TECHNOLOGY AND SECURITY POLICIES REVIEW**

The Board of Supervisors' (Board) Information Technology (IT) and Security Policies (Policies) require all County departments to comply with established Countywide IT security standards to help ensure proper controls over County IT resources. As required by Board Policy 6.108, we are reviewing County departments' compliance with the Policies.

We have completed a review of the Department of Mental Health's (DMH or Department) compliance with the Policies and related County standards. In Fiscal Year 2014-15, DMH reported 18 critical IT systems, including 16 that manage protected health information (PHI). DMH also reported approximately 5,900 IT devices, such as desktop computers, laptops, and servers. Our review included testing DMH's systems access controls, IT equipment controls, antivirus and encryption software management, and equipment disposition.

Results of Review

Our review disclosed that DMH needs to improve its controls over areas such as systems access controls, IT equipment controls, antivirus and encryption software management, and equipment disposition. The following are examples of areas for improvement:

- **Inappropriate Systems Access Rights** – DMH needs to restrict unneeded user access rights to sensitive/confidential information, as required by Board Policy 3.040. We reviewed user access rights to PHI in the Integrated Behavioral Health Information System (IBHIS), DMH's primary electronic health record system, and in Microsoft Active Directory (AD), DMH's electronic access management platform for several of DMH's critical systems. We noted a total of 133 users remained active in IBHIS and AD for up to two years after terminating service from DMH, including 64 users with access to PHI. We verified that none of the 64 accounts with access to PHI were accessed after the employees' termination dates.

  We also reviewed 15 current DMH employees with access to PHI in IBHIS, and noted that three (20%) never needed their IBHIS system access. We verified that none of the three employees used their IBHIS access.

  DMH's attached response indicates they are developing a report to assist with deactivating stale user accounts, and is locking inactive user accounts after 90 days. DMH management also told us that they have deactivated all unneeded user accounts identified in the audit.

- **Access Control Procedures** – DMH management needs to improve its processes for authorizing, restricting, and monitoring access to Departmental systems. Specifically, we noted that:

  - DMH's Human Resources Bureau (HRB) does not always notify the Department's Chief Information Office Bureau (CIOB) of employee terminations timely, as required by DMH Policy 601.03. As a result, CIOB staff cannot always restrict systems access timely.
  - IBHIS access administrators do not document approvals for the user access profiles that they assign and change in IBHIS, as required by County Fiscal Manual (CFM) Section 8.7.4.2.
  - DMH management does not periodically review IBHIS and AD user access levels to ensure that access is authorized and restricted based on users' job duties, as required by CFM Section 8.7.4.2.

  These weaknesses increase the risk that individuals could gain unauthorized and undetected access to DMH systems/data.

  DMH's attached response indicates that their HRB now notifies CIOB of employee terminations within required timeframes, and the IBHIS Team has developed an authorization form to document approvals for IBHIS access levels. In addition, DMH indicates that they will require Program Heads to periodically review and validate all of their employees' user access levels.

- **User Authentication** – DMH needs to remind staff to never share or write down, in an unsecured location, system logon identifications (ID) and passwords, as required by Board Policy 6.101. We observed one employee share her network logon ID with a colleague at the colleague's request, and observed another employee's logon ID and password written down and taped to a computing device.

  DMH's attached response indicates that they have increased the frequency of password security reminders they send to staff. In addition, DMH Program Heads will now periodically review Board Policy 551.03 "Workstation Use and Security" during staff meetings, DMH's Privacy Officer will train staff on password security guidelines, and DMH's Information Security Team will monitor for password security violations during facility walkthroughs.

- **Equipment Control** – DMH needs to improve controls over IT equipment, as required by Board Policy 6.106. We noted that 20 (33%) of the 60 IT equipment items reviewed were not accurately accounted for in DMH's inventory records. The items reflected an incorrect status, location, and/or custodian. In addition, two (3%) of the 60 devices were missing a County property tag, and nine (15%) of the 60 devices were not actively being used by staff and need to be evaluated for reassignment or disposal.

  DMH's attached response indicates that they will update their equipment inventories to correct the inaccuracies noted in the audit. DMH is also updating their policy to require staff to report computer equipment that is unassigned or unused for over a certain amount of time, and managers and supervisors are required to communicate all equipment changes timely to ensure equipment inventories are updated.

- **Computer Encryption** – DMH needs to ensure all workstations are encrypted, and needs to periodically monitor computer encryption status, as required by Board Policy 6.110. We reviewed 58 computing devices and noted two (3%) desktops that did not have encryption software installed. While DMH configured all 58 computer devices to prevent users from saving data to the hard drive, DMH management must still ensure that all software on portable computers and workstations is protected with encryption, as required.

  In addition, DMH IT staff do not monitor computer encryption due to lack of an encryption reporting feature within their current encryption management software. DMH is in the process of implementing a new encryption management solution that should allow IT staff to produce and monitor computer encryption reports.

  DMH's attached response indicates that they are transitioning to a new encryption solution that will improve their ability to report on computer encryption. Upon implementation, DMH indicates they have established a new process to monitor and

investigate computers that appear in their AD environment but do not appear on an encryption report.

- **Antivirus Software** – DMH needs to ensure that computers are protected with up-to-date antivirus software, as required by Board Policy 6.102. We reviewed a DMH antivirus report and noted that 51 (1%) of the 4,226 computing devices had an outdated antivirus software version and/or definitions. We also could not determine whether another 1,645 computers had any antivirus software because they had not recently connected to DMH's network and were not captured on the antivirus report. We inspected 58 computers, including 39 that were not on the antivirus report, and noted that 22 (38%) did not have current antivirus software installed, with versions or definitions as old as May 2012. Outdated antivirus software is less effective at preventing malicious attacks. This increases the risk that intruders could gain unauthorized access to the Department's network and to sensitive/confidential information.

  DMH's attached response indicates that they have fine-tuned their Antivirus Management Console to provide more accurate reports and better protection to account for devices that were not listed on the previous reports.

- **Hard Drive Destruction** – DMH needs to document that every device hard drive is erased before disposal, as required by Board Policy 6.112. We noted that DMH generally removes and destroys hard drives before disposing of computing devices. However, DMH's hard drive destruction records do not include enough information to match each destroyed hard drive to the device from which it was removed (i.e., the make, model, and serial number, or the property tag number of the computer or server). This lack of information makes it impossible to verify that every device had its hard drive destroyed.

  We also observed 15 computing devices that had passed through DMH's hard drive destruction process and were about to be disposed. We noted that DMH IT staff did not remove and destroy one (7%) computer hard drive and the associated software.

  DMH's attached response indicates that they will enhance their hard drive destruction records by recording the serial number of the hard drive destroyed along with the serial number of the computer it was removed from. DMH also indicates they will require their IT technicians to remove computer cases from devices when they are being prepared for salvage. This will provide a clear view of any hard drives left in a computer device so that technicians can remove and destroy them prior to salvage.

Details of these and other findings and recommendations are included in Attachment I.

Review of Report

We discussed our report with DMH management. The Department's attached response (Attachment II) indicates general agreement with our findings and recommendations, and describes actions that they have taken or plan to take to implement our recommendations.

We thank DMH management and staff for their cooperation and assistance during our review. If you have any questions please call me, or your staff may contact Robert Smythe at (213) 253-0100.

JN:AB:PH:RS:MP

Attachments

c: Sachi A. Hamai, Chief Executive Officer
Robin Kay, Ph.D., Acting Director, Department of Mental Health
Dr. Robert Pittman, Chief Information Security Officer, Chief Executive Office
Public Information Office
Audit Committee

DEPARTMENT OF MENTAL HEALTH
INFORMATION TECHNOLOGY AND SECURITY POLICIES REVIEW

Background

The Board of Supervisors' (Board) Information Technology (IT) and Security Policies (Policies) require all County departments to comply with minimum IT security standards. The Policies help protect County IT assets and ensure the confidentiality and integrity of systems and data. As required by Board Policy 6.108, we are reviewing County departments' compliance with the Policies.

We have completed a review of the Department of Mental Health's (DMH or Department) compliance with the Policies and related County standards. In Fiscal Year 2014-15, DMH reported 18 critical IT systems, including 16 that store/manage protected health information (PHI). DMH also reported approximately 5,900 IT devices, such as desktop computers, laptops, and servers. Our review included testing DMH's systems access controls, IT equipment controls, antivirus and encryption software management, and equipment disposition.

Systems Access Controls

Board Policy 3.040 requires departments to safeguard personal and confidential information within their IT systems. County Fiscal Manual (CFM) Section 8.7.4.2 also requires departments to limit unneeded systems access by immediately updating user access rights when employees terminate or change job duties, and by periodically reviewing the propriety of users' access levels. DMH's Chief Information Office Bureau (CIOB) oversees system access administration for the Department.

Inappropriate Access Rights

We reviewed electronic access rights to personal and confidential information for two of the 18 critical IT systems that DMH reported: the Integrated Behavioral Health Information System (IBHIS) and Microsoft Active Directory (AD).

DMH uses IBHIS as its primary health record system to manage clients' clinical and billing records, and uses AD as its enterprise authentication system to manage access to multiple critical IT services, such as the Treatment Authorization Request System, Access Center Contact Manager, and the Service Request Automation Service Catalog, which all store and manage PHI.

We noted the following inappropriate user access rights for IBHIS and AD:

- 89 IBHIS and 44 AD users remained active in the systems for up to two years after terminating service from DMH, including 64 users with access to view or modify PHI. We reviewed IBHIS and AD activity reports and noted that none of the 64 terminated user accounts were accessed after the employees' termination dates.

- We reviewed 15 current employees with access to PHI in IBHIS, and noted that three (20%) never needed their access. These three employees had unneeded access to PHI for up to eight months. However, we verified that the employees never used their access.

DMH needs to immediately deactivate user access for the terminated employees noted in our review, and for the current DMH employees who do not need access to IBHIS.

Recommendation

1. **Department of Mental Health management immediately deactivate user access for the terminated employees noted in our review, and for the current employees who do not need access to the Integrated Behavioral Health Information System.**

Access Control Procedures

We noted weaknesses in DMH's controls over user access administration for IBHIS and AD that contributed to the inappropriate access rights noted above. Specifically:

- DMH's Human Resource Bureau (HRB) does not always notify CIOB of employee terminations within one business day of the termination, as required by DMH Policy 601.03. Specifically, we reviewed HRB notifications for ten terminated DMH employees. For six (60%) of the ten, HRB notified CIOB an average of 40 days after the employee terminated. For four (40%) of the ten, HRB could not support that they ever notified CIOB. Notification delays increase the risk that terminated employees will not be deactivated timely from DMH systems.

- IBHIS access administrators do not document approvals for the user access profiles that they assign and change in the system, as required by CFM 8.7.4.2. DMH has several IBHIS Local User Administrators (LUAs) at each office who add and change user access profiles based on informal requests that they do not retain, such as e-mails from employees or their managers. The lack of a documented approval increases the risk that LUAs could make unauthorized access changes, and makes it difficult for DMH management to monitor whether IBHIS access levels are authorized.

- DMH management does not periodically review AD and IBHIS user access to ensure that access levels are authorized and continue to be consistent with employees' job duties, as required by CFM Section 8.7.4.2. This increases the risk that unauthorized or inappropriate systems access will not be detected timely.

- IBHIS access administrators do not always require users to sign a User Security Agreement (Agreement) when they receive access to IBHIS, as required by DMH Policy 550.04. Specifically, three (20%) of the 15 IBHIS users reviewed with access

to PHI did not sign an Agreement to acknowledge their responsibility to protect County IT resources and data.

To ensure appropriate access to and use of County IT resources, DMH management needs to ensure that HRB notifies the CIOB of employee terminations within the timeframes required by Department policy. Management also needs to require IBHIS LUAs to document management approval for the user access levels they assign and change, periodically review systems access to ensure that access levels are authorized and continue to be appropriate, and ensure that all IBHIS users have completed an Agreement.

Recommendations

Department of Mental Health management:

2. **Ensure that Department of Mental Health's Human Resources Bureau notifies the Chief Information Office Bureau of employee terminations within the timeframes required by Department policy.**

3. **Require Local User Administrators for the Integrated Behavioral Health Information System to document management approval for the user access levels they assign and change.**

4. **Periodically review systems access to ensure that all users' access levels are authorized and continue to be appropriate for their job duties.**

5. **Ensure that all Integrated Behavioral Health Information System users have completed a User Security Agreement.**

User Authentication

Board Policy 6.101 requires County IT users to protect the integrity of computer authentication mechanisms that they are assigned. For example, users must not share their unique computer logon identifications (ID) and passwords, or write them down in an unsecured location.

We noted that DMH IT users do not always protect their systems access credentials. Specifically, we observed one employee share her network logon ID and password with a colleague at the colleague's request, and observed another employee's logon ID and password written down and taped to a computer device.

Recommendation

6. **Department of Mental Health management remind staff to never share system logon identifications and passwords, or write them down in an unsecured location.**

IT Equipment Control

Board Policy 6.106 requires departments to establish safeguards over IT equipment, including assigning IT equipment to custodians to establish accountability, and ensuring all IT equipment has a property tag affixed to identify it as County property.

We reviewed 60 IT equipment items at ten DMH offices, and noted weaknesses in equipment oversight. These weaknesses could result in DMH computers and data becoming missing or stolen without being detected. Specifically:

- **Inaccurate Tracking** – 20 (33%) of the 60 items reviewed have an inaccurate custodian, location, equipment status, or equipment description recorded on DMH's equipment listing. This includes several items that had been salvaged but were never deactivated on DMH's equipment listing.

- **Equipment Assignments** – Nine (15%) of the 60 equipment items reviewed are not actively being used. This includes three employees who indicated they do not use their laptop on a regular basis because they already have a desktop computer. We also noted six desktop computers located in vacant cubicles that had not been reassigned or used for over six months. DMH management indicated that some offices have a laptop pool where staff can check out a laptop when needed. However, laptop pools were not in place at the offices where we noted unneeded laptops.

  To avoid over-purchasing IT equipment and software, DMH must maximize how it assigns and uses existing resources. DMH needs to evaluate existing staff computer assignments, consider expanding the laptop pool program to all offices, and transfer or salvage unneeded items.

- **Property Tags** – Two (3%) of the 60 IT devices available for review did not have property tags to identify the devices as County property. Though an asset number was assigned to the equipment when placed in service, DMH could not determine if the tags had been removed, fallen off, or were never affixed to the devices.

Staff in the CIOB Asset Management section, who are responsible for distributing the Department's IT assets and maintaining equipment lists, indicated that equipment lists are not accurate in part because employees and managers at field offices do not always notify them of equipment assignment changes that impact the IT inventory.

Recommendations

Department of Mental Health management:

7. **Update the Department's equipment inventory for the inaccuracies noted in our review.**

8. **Evaluate staff computer assignments, consider expanding the laptop pool program to all offices, and transfer or salvage unneeded items.**

9. **Ensure a County property tag is attached to all County equipment.**

10. **Remind office managers to immediately communicate all staffing and equipment assignment changes to the Asset Management section.**

Physical Security

Board Policy 6.106 requires departments to physically safeguard IT resources from tampering, damage, theft, or unauthorized physical access. In addition, DMH Policy 551.03 requires staff to secure computer workstations located in open areas to deter unauthorized movement. These controls help prevent equipment and data loss.

We visited ten DMH offices and noted DMH staff do not always secure unattended computer equipment. Specifically, 23 (38%) of the 60 devices reviewed were not securely stored or locked to a permanent fixture when left unattended. One of the unsecured items was a laptop that an employee stored in her car, which is prohibited by County IT Security Guideline 110.01.

DMH CIOB indicated that they assign cable locks to employees so that they can secure unattended portable computers such as laptops. However, some employees reported that they never received cable locks. DMH needs to remind all staff not to leave laptop computers in their car, and to secure unattended computer equipment. They also need to evaluate issuing additional cable locks to assist staff in securing portable computers.

Recommendations

Department of Mental Health management:

11. **Remind all staff not to leave laptop computers in their car, and to lock/secure unattended computer equipment.**

12. **Evaluate issuing additional cable locks to staff to assist in securing portable computers.**

Encryption Software

Board Policy 6.110 requires departments to encrypt all County owned portable computers (e.g., laptops). In December 2014, the Chief Information Office (CIO) issued Technology Directive 14-04 to extend the encryption requirement to all County owned workstations (e.g., desktop computers). Encryption helps render data unreadable if a computer is lost or stolen, and protects against unauthorized disclosure of personal/confidential information. While DMH configures its computer devices to prevent users from saving data to the hard drive, DMH management must still ensure that all software on portable computers and workstations is protected with encryption, as required.

We reviewed 58 DMH computer devices and noted two (3%) desktop computers did not have encryption software installed. Although DMH IT management reported to the CIO in September 2015 (prior to our audit), that they had fully implemented workstation encryption, DMH IT staff indicated that these desktops were overlooked during implementation of Technology Directive 14-04.

We also noted that DMH can improve its encryption documentation. Specifically, DMH could not document that they encrypted over 1,000 of their computer devices. This occurred because DMH's encryption management software lacks encryption documentation and reporting features. DMH management indicated that they are in the process of deploying a new encryption solution that will allow them to fully document that all devices are encrypted. Upon full implementation of this solution, DMH management should ensure staff periodically monitor the encryption status of all portable computers and workstations.

Recommendation

13. Department of Mental Health management periodically monitor to ensure that all portable computers and workstations are encrypted, and ensure that the encryption is documented.

Antivirus Software

Board Policy 6.102 requires departments to ensure they have functioning up-to-date antivirus software protection for all County computers. Departments must update antivirus software regularly to protect against the most current threats.

We reviewed a DMH antivirus report and noted that 51 (1%) of the 4,226 computing devices had outdated antivirus versions or definitions. We also noted at least 1,645 DMH computers do not appear on the antivirus report because they had not recently connected to the Department's network. Therefore, we reviewed 58 computer devices, including 39 that did not appear in the antivirus report, and noted that all devices have antivirus software. However, 22 (38%) devices did not have the most current antivirus software version and definitions, with one device having a version as old as May 2012.

DMH IT staff indicated that the outdated antivirus software and definitions were due to the infrequent network connections from users. DMH management needs to ensure that staff update their antivirus protection by regularly connecting their assigned computers to the Department's network, or to the appropriate antivirus website.

Recommendation

14. Department of Mental Health management ensure that staff update their antivirus protection by regularly connecting their assigned computers to the Department's network, or to the appropriate antivirus website.

Hard Drive Destruction

Board Policy 6.112 requires departments to render all data and software from computer hard drives unreadable and unrecoverable before disposing of the devices from County inventory. To accomplish this, DMH IT staff removes and destroys computer hard drives before disposing of every computing device.

We noted that DMH's hard drive destruction records do not include enough information to identify the device from which each hard drive was removed (i.e., the make, model, and serial number, or the property tag number of the computer or server). This lack of information makes it impossible for management to verify that every device had its hard drive destroyed. To ensure that DMH can document hard drive destruction for every device, IT staff need to document the device make, model, and serial number, or the property tag number, for every hard drive destroyed.

In addition, we reviewed 15 computers located at a DMH warehouse that had passed through DMH's hard drive destruction process and were about to be disposed. We noted that one (7%) computer still had a hard drive connected that was never removed and destroyed. If not detected, this hard drive could have been donated without removing the associated County software. DMH management needs to remind IT supervisors and staff to verify that all computer hard drives are removed and destroyed prior to disposal.

Recommendations

Department of Mental Health management:

15. Require information technology staff to document the device make, model, and serial number, or the device property tag number, for every hard drive destroyed.

16. Remind information technology supervisors and staff to verify that all computer hard drives are removed and destroyed prior to disposal.

LOS ANGELES COUNTY DEPARTMENT OF MENTAL HEALTH
550 S. VERMONT AVE., LOS ANGELES, CA 90020 HTTP://DMH.LACOUNTY.GOV

ROBIN KAY, Ph.D.
Acting Director
DENNIS MURATA, M.S.W.
Acting Chief Deputy Director
RODERICK SHANER, M.D.
Medical Director

September 20, 2016

TO: John Naimo
Auditor-Controller

FROM: Robin Kay, Ph.D.
Acting Director

SUBJECT: **RESPONSE TO THE AUDITOR-CONTROLLER'S DEPARTMENT OF MENTAL HEALTH – INFORMATION TECHNOLOGY AND SECURITY POLICIES REVIEW**

This is in response to the Auditor-Controller's (A-C) recommendations resulting from the review of the Department of Mental Health's (DMH or Department) Information Technology and Security Policies conducted by your staff. We agree with your recommendations and appreciate the opportunity to work with your staff in identifying areas needing improvement. The specific actions undertaken are outlined in this response.

System Access Controls

Recommendation 1:

DMH management immediately deactivates user access for the terminated employees noted in our review and for the current employees who do not need access to the Integrated Behavioral Health Information System (IBHIS).

DMH's Response to Recommendation 1:

DMH agrees with this recommendation and anticipates full implementation by December 31, 2016.

A guidelines document was created and distributed in August 2016 to further assist Program Managers and Local User Administrators (LUA) in selection of user roles to assigned staff.

A report is in development that will identify any needed modifications to user roles. This report will be run on a regular basis (frequency to be determined) by the LUA. Once this report is placed in production use, the information will be utilized to deactivate all non-active or stale user accounts.

To further mitigate against non-active or stale user accounts, those that have surpassed 90 days (that is, any account that has not been accessed during a 90-day period) are automatically locked. The user must contact the LUA in order to unlock the user account and have the password reset. This process has been in place since production use of IBHIS effective January 27, 2014.

Recommendation 2:

Ensure that DMH's Human Resources Bureau (HRB) notifies the Chief Information Office Bureau (CIOB) of employee terminations within the time frames required by Department policy.

DMH's Response to Recommendation 2:

DMH agrees with this recommendation. As of August 1, 2016, HRB is notifying CIOB within the time frames required by Department's policy.

Recommendation 3:

Require LUA for the IBHIS to document management approval for the user access levels they assign and change.

DMH's Response to Recommendation 3:

DMH agrees with the recommendation. The DMH IBHIS Team has developed a User Role Authorization Form that must be submitted by an approved Program Manager or his/her designee to the LUA. This new process was launched on August 1, 2016, with a limited grace period, until September 30, 2016, for compliance to the new process and procedures for any staff changes, transfers, and termination of IBHIS users. This includes completion and submission of the User Role Authorization Form for all current IBHIS users and new staff prior to gain access to IBHIS.

Recommendation 4:

Periodically review systems access to ensure that all users' access levels are authorized and continue to be appropriate for their job duties.

DMH's Response to Recommendation 4:

DMH agrees with this recommendation and anticipates full implementation by December 31, 2016.

A report was developed which identifies the status and role of all active users under each Program Head. This report will be run on a regular basis (frequency to be determined) and reviewed by Program Heads. Program Heads or their designees will validate and re-authorize all users' access levels. LUAs will then deactivate all

non-active or stale user accounts and modify others' access levels as approved by the Program Head.

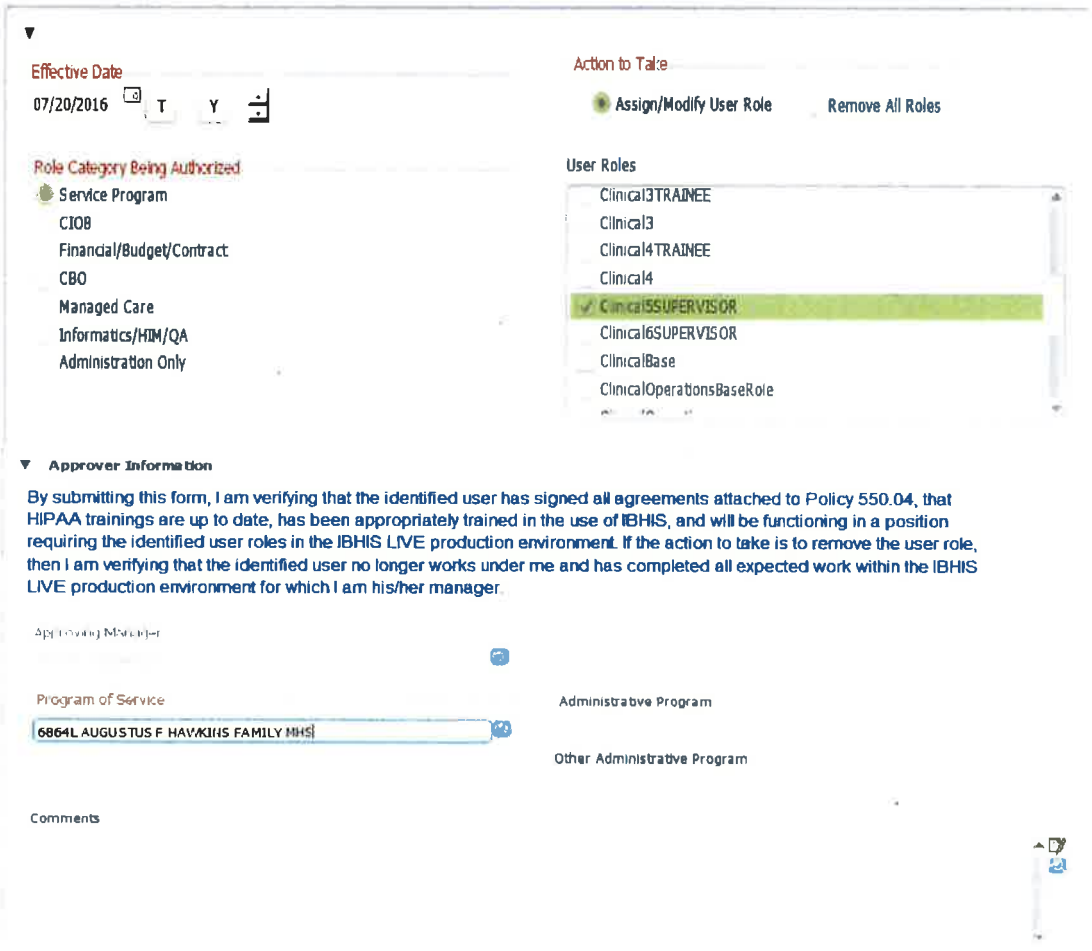
Recommendation 5:

Ensure that all IBHIS users have completed a User Security Agreement.

DMH's Response to Recommendation 5:

DMH agrees with this recommendation. As described above in response to Recommendation 3, the User Role Authorization Form was implemented on August 1, 2016, and will address a number of recommendations including documentation of User Access within IBHIS that will compliment other types of User Security Agreements such as the Acceptable Use and Confidentiality Agreement and Health Insurance Portability and Accountability Act (HIPAA) compliance policies.

Below are partial screen shots of the IBHIS User Role Authorization Form:



Recommendation 6:

DMH management reminds staff to never share system logon identifications and passwords, or write them down in an unsecured location.

DMH's Response to Recommendation 6:

DMH agrees with this recommendation. For the past eight years, DMH has sent security reminders by email to all DMH workforce members on a monthly basis. The reminders are comprised of various topics, one of which is not to share or write down passwords. The password topic use to be sent once a year. Effective January 1, 2016, CIOB commenced sending the password topic as often as twice per month or at least six times a year.

In addition, effective January 1, 2016, every time a password violation is identified, DMH Program Heads are reminded to review Board Policy 551.03 "Workstation Use and Security" regularly in their staff meetings and emphasize Sections 2.1.4.1.2, 3, and 4 that prohibit sharing of passwords and writing them down; the DMH Privacy Officer communicates the password guidelines during all trainings; and, the DMH Information Security team includes password sharing and writing as part of its facility audit risk assessment procedures so that during site walkthroughs, random workforce and management will be tested (inspectors will ask for workers' passwords and document their reactions).

IT (Information Technology) Equipment Control

Recommendation 7:

Update the Department's equipment inventory for the inaccuracies noted in our review.

DMH's Response to Recommendation 7:

DMH agrees with the recommendation. Notebooks are assigned to individuals and recorded as such. Inventory for desktop systems are maintained by Altiris software which provides the custodian information. DMH will update the inventory to correct inaccuracies.

Recommendation 8:

Evaluate staff computer assignments, consider expanding the laptop pool program to all offices, and transfer or salvage unneeded items.

DMH's Response to Recommendation 8:

DMH agrees with the recommendation. CIOB has been evaluating computer assignments as requests for additional computers are submitted via our service catalog

and as computers are due for replacement at end of life cycle. In addition, as technicians perform computer break/fix work and see unused devices, they speak with the device custodian (site program managers are designated custodians of all site pooled or unused devices) to reexamine the need for the device.

DMH is taking action to further maximize how it assigns and uses computer resources. DMH is currently reviewing and updating all IT related policies and will add content that will require designated computer custodians to report any computers that are unassigned or unused for over a certain amount of time (to be determined during policy revision) to CIOB for processing. The policy document revision will be completed no later than June 30, 2017. Prior to that, DMH will remind these custodians to periodically review their staff's computer equipment assignments to ensure they are appropriate and contact CIOB for required changes. CIOB will then change device assignments, including moving to use additional pooled devices if appropriate, or transferring or salvaging unneeded devices.

Recommendation 9:

Ensure a County property tag is attached to all County equipment.

DMH's Response to Recommendation 9:

DMH agrees with the recommendation. As of September 1, 2016, CIOB Asset Management Section began attaching County property tags on equipment upon receipt.

Recommendation 10:

Remind office managers to immediately communicate all staffing and equipment assignment changes to the Asset Management Section.

DMH's Response to Recommendation 10:

DMH agrees with the recommendation. DMH management is aware that any computing equipment that is not needed will be returned back to CIOB for re-distribution or salvage. Management is also aware that any computing equipment change must be communicated to CIOB. DMH Executive Management will require all DMH managers and supervisors to comply with this requirement. To resolve the conflict between the need to assure equipment is not sitting idle for long periods and to provide necessary equipment to new staff coming onboard promptly, DMH will continue to look for ways to improve the service process.

Physical Security

Recommendation 11:

Remind all staff not to leave laptop computers in their car and to lock/secure unattended computer equipment.

DMH's Response to Recommendation 11:

DMH agrees with the recommendation. Starting in August 2016, DMH added a new security reminder that includes specific instructions about staff's responsibilities for physically safeguarding their assigned computing devices. This reminder points out that portable devices must be secured with the provided lock cable to a desk or furniture during business hours. For after hours and overnights, the notebook must be locked in an enforced cabinet or carried home. It also indicates that during transportation, the devices must be stored in the trunk of their vehicle and prohibits storing of computing equipment in the vehicle overnight, instead requires the assignee to carry the device inside his/her residence.

Additionally, DMH Program Heads have been asked to survey their respective facilities and identify all the computing devices that are currently not secured by a lockable mechanism. The survey must then be submitted to DMH Helpdesk so that a technician is tasked to lock those computers.

To compliment the security reminder, DMH Information Security is reviewing the IT policies and plans to add applicable language that will hold the workforce responsible and discipline those that neglect or choose not to cooperate with the guidelines.

Recommendation 12:

Evaluate issuing additional cable locks to staff to assist in securing portable computers.

DMH's Response to Recommendation 12:

DMH agrees with the recommendation. When a user is approved to receive a notebook, a locked cable is always allocated to accompany the device. The cable is placed in the carrying case among the other accessories. When picking up, the user verifies the list of items and signs for them. No laptop is distributed without this cable. The above mentioned security reminder also prompts users that have misplaced or are unable to find their notebook's security cable to individually contact DMH Helpdesk and request a replacement immediately.

To compliment the security reminder, DMH Information Security is reviewing the IT policies and plans to add applicable language that will hold the workforce responsible and discipline those that neglect or choose not to cooperate with the guidelines.

Encryption Software

Recommendation 13:

DMH management periodically monitors to ensure that all portable computers and workstations are encrypted and ensure that the encryption is documented.

DMH's Response to Recommendation 13:

DMH agrees with the recommendation. DMH Information Security has created a new workflow that includes one-to-one comparison of all DMH Active Directory (AD) Desktop Computers with a report that could be generated through WinMagic listing all successfully encrypted devices. Any AD object in this list for which a match is not found will be considered risky and will be disabled immediately. An assignment will then be created for a technician to visit the device and apply correction or re-image. Please note that a disabled device will not allow a user to connect to DMH domain and resources. By this action, the potential risks are mitigated and remediated once the issue is corrected by the technician.

The WinMagic vendor was also consulted and asked to develop a feature that will perform the above described manual process and report all the existing devices that are unencrypted. This enhancement, which will simplify and increase the efficiency of the existing process, is promised to be included in the next built scheduled for the fourth quarter of 2016.

The noted 19 percent of devices are protected by an older encryption solution Pointsec. Although the tool does not have a graphical display console, a manual process can tally all the Pointsec decryption keys that match each notebook's identity. We agreed that Pointsec reporting facility is not robust, but when it was selected by County Data Security, it was the best option available at the time. DMH has been transitioning from Pointsec to WinMagic for encryption. DMH has a project underway to upgrade all our desktop and notebook computers to Windows 10. During this process every device will be touched and WinMagic will be installed. We expect this project to be completed by the middle of Fiscal Year 2017-18.

Antivirus Software

Recommendation 14:

DMH management ensures that staff updates their antivirus protection by regularly connecting their assigned computers to the Department's network or to the appropriate antivirus website.

DMH's Response to Recommendation 14:

DMH agrees with the recommendation. DMH currently uses Symantec Endpoint protection to manage its antivirus software. Since the audit, the Symantec Antivirus Management Console has been fine tuned to provide more accurate reports and better protection to account for devices that were not listed on the previous reports.

Hard Drive Destruction

Recommendation 15:

Require IT staff to document the device make, model, and serial number, or the device asset tag number for every hard drive destroyed.

DMH's Response to Recommendation 15:

DMH agrees with the recommendation. It is DMH's procedure to scan the serial number of the hard drive to be destroyed. A report created from the scanned serial numbers, and the certificates of destruction provided by the vendor are then retained for our record.

Effective October 1, 2016, DMH will begin recording both the serial number of the hard drive and the serial number of the Personal Computer.

Recommendation 16:

Remind IT supervisors and staff to verify that all computer hard drives are removed and destroyed prior to disposal.

DMH's Response to Recommendation 16:

Effective March 30, 2016, DMH is requiring all technicians to have all equipment cases removed in order to have a clear view of any hard drive left behind in the devices before being salvaged. This practice will be added to relevant CIOB policy and procedure. All supervisors and staff that come into contact with computer hard drives have been reminded and will be periodically reminded again.

If you have any questions, please call me, or your staff may contact Margo Morales, Administrative Deputy, at (213) 738-2891.

RK:MM:KVS:ag

c: Karen Van Sant
Margo Morales